



DIRECT DIAL:

512.469.6177

aaron.weiss@tklaw.com

THOMPSON & KNIGHT

LLP

ATTORNEYS AND COUNSELORS

1200 SAN JACINTO CENTER
98 SAN JACINTO BOULEVARD
AUSTIN, TEXAS 78701-4081

(512) 469-6100
FAX (512) 469-6180
www.tklaw.com

#4 2121
12.13.02

AUSTIN
DALLAS
FORT WORTH
HOUSTON
MONTERREY, MEXICO

RECEIVED

DEC 03 2002

Technology Center 2100

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231, on the date below:

11-27-02

Date

A. Weiss

Signature

Commissioner for Patents
Washington, DC 20231

RE: SN 10/068,294 "RING ARITHMETIC METHOD, SYSTEM, AND APPARATUS"- George Robert Blakley
(Our File No. 501143.000008)

Sir:

Enclosed for filing in connection with the above-referenced patent application are:

1. Information Disclosure Statement (PTO/SB/08A); 3 pages
2. Copies of documents A1 – A13; C1 – C20 cited in the Information Disclosure Statement; and
3. Return receipt postcard.

In accordance with 37 C.F.R. §§ 1.97(g),(h), the enclosed Information Disclosure Statement is not to be construed as a representation that a search has been made, and is not to be construed to be an admission that the information cited is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

The Information Disclosure Statement is being filed prior to the receipt of a first Office Action reflecting an examination on the merits, and hence is believed to be timely filed in accordance with 37 C.F.R. § 1.97(b).

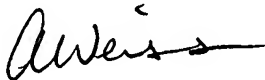
No fees are believed to be due in connection with the filing of these documents. However, should any fees under 37 C.F.R. §§ 1.16 to 1.21 be deemed necessary for any reason relating to

Commissioner for Patents
November 27, 2002
Page 2

the enclosed materials, the Commissioner for Patents is hereby authorized to deduct said fees from Thompson & Knight, L.L.P.'s Deposit Account No. 20-0821/501143.000008/AAW.

Applicants respectfully request that the listed documents be made of record in the present case. Please date stamp and return the enclosed postcard evidencing receipt of these materials.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "A. Weiss", followed by a horizontal flourish.

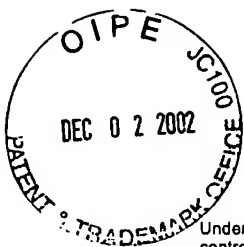
Aaron A. Weiss
Reg. No. 46,163

AAW:ce
Encl.

PTO/SB/08A (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Examiner Signature	Date Considered
-----------------------	--------------------

¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.



PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Complete if Known	
		Application Number	10/068,294
		Filing Date	February 5, 2002
		First Named Inventor	Blakley, George Robert
		Group Art Unit	2121
		Examiner Name	
Sheet 2	of 3	Attorney Docket Number	501143.00008

RECEIVED

DEC 09 2002

Technology Center 2100

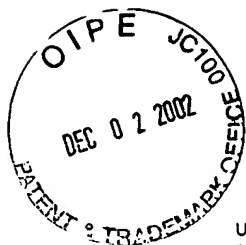
OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	C1	MENEZES, A.J., et al "Efficient Implementation" from the Handbook of Applied Cryptography, (Boca Raton, CRS Press, 1997), pp. 591-607.
	C2	DIMITROV, V. and COOKLEV, T., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics" IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995.
	C3	KOC, C.K. and HUNG, C.Y., "Carry-Save Adders for Computing the Product AB Modulo N" Electronics Letters, Vol. 26, No. 13, (June 21, 1990), pp. 899-900
	C4	FREKING, W. L. and PARHI, K.K., "Montgomery Modular Multiplication and Exponentiation in the Residue Number System" Proc. 33rd Asilomar Conf. Signals Systems and Computer, October 1999, pp. 1312-1316.
	C5	TENCA, A.F. and KOC, C.K., "A Scalable Architecture for Montgomery Multiplication" in: KOC, C.K. and PAAR, C., Cryptographic Hardware and Embedded Systems, CHES 99, Lecture Notes in Computer Science, No. 1717, 1998, New York, NY: Springer-Verlog, 1999.
	C6	KOC, C.K. and ACAR, T., "Montgomery Multiplication in GF (2k)" 3rd Annual Workshop on Selected Areas in Cryptography, (August 15-16, 1996), pp. 95-106.
	C7	BAJARD, J.C., et al "An RNS Montgomery Modular Multiplication Algorithm" IEEE Transactions on Computer, Vol. 47, No. 7, (July 1998), pp. 766-776.
	C8	ELDRIDGE, S.E., "A Faster Modular Multiplication Algorithm" International Journal of Computer Math, Vol. 40, (1991), pp. 63-68.
	C9	BOSSALAERS, A., et al "Comparison of Three Modular Reduction Functions" In Douglas R. Stinson, editor, Advances in Cryptology - CRYPTO '93, Vol. 773 of Lecture Notes in Computer Science, (August 22-26, 1993), pp. 166-174.
	C 10	MONTGOMERY, P.L., "Modular Multiplication Without Trial Division" Mathematics of Computation, Vol. 44, No. 170 (April 1985), pp. 519-521.
	C 11	KOC, C.K., et al "Analyzing and Comparing Montgomery Multiplication Algorithms" IEEE Micro, Vol. 16, Issue 3, (June 1996), pp. 26-33.

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>		Complete if Known	
		Application Number	10/068,294
		Filing Date	February 5, 2002
		First Named Inventor	Blakley, George Robert
		Group Art Unit	2121
		Examiner Name	
Sheet 3	of 3	Attorney Docket Number	501143.000008

RECEIVED

DEC 03 2002

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	C 12	KORNERUP, P., "High-Radix Modular Multiplication for Cryptosystems" Department of Mathematics and Computer Science, (1993), pp. 277-283.	
	C 13	SUNAR, B. and KOC, C.K., "An Efficient Optimal Normal Basis Type II Multiplier" Brief Contributions, IEEE Transactions on Computers, Vol. 50, No. 1, (January 2001), pp. 83-87.	
	C 14	KOC, C.K., "Comments on 'Residue Arithmetic VLSI Array Architecture for Manipulator Pseudo-Inverse Jacobian Computation'" Communications, IEEE Transactions on Robotics and Automation, Vol. 7, No. 5, (October 1991), pp. 715-716.	
	C 15	SAVAS, E. and KOC, C.K., "The Montgomery Modular Inverse-Revisited" IEEE Transactions on Computers, Vol. 49, No. 7, (July 2000), pp. 763-766.	
	C 16	WALTER, C.D., "Montgomery's Multiplication Technique: How to Make it Smaller and Faster" in Cryptographic Hardware and Embedded Systems - CHAS 1999, C. Paar (Eds.), K. Ko, Ed. 1999, Springer, Berlin Germany, pp.61-72.	
	C 17	OH, H. and MOON, J., "Modular Multiplication Method" IEE Proc.-Comput. Digit. Tech., Vol. 145, No. 4, (July 1998), pp. 317-318.	
	C 18	BLUM, T., "Modular Exponentiation on Reconfigurable Hardware" Master's thesis, ECE Department, Worcester Polytechnic Institute, Submitted to Faculty 1999-04-08, Published May 1999. Retrieved from the Internet <URL: http://www.wpi.edu/pubs/ETD/Available/etd-090399-090413/unrestricted/blum.pdf >.	
	C 19	MARWEDEL, P., et al. "Built in Chaining: Introducing Complex Components into Architectural Synthesis." April 1996. Proceedings of the ASP-DAC, 1997. [online]. Retrieved from the Internet <URL: http://eldorado.uni-dortmund.de:8080/FB4/Is12/forshung/1997/aspdac/aspacPDF >.	
	C 20	TIOUNTCHIK, A., and TRICHINA, E., "RSA Acceleration with Field Programmable Gate Arrays" Lecture Notes in Computer Science, Vol. 1587, pp.164-176. Retrieved from the Internet: <URL: http://citeseer.nj.nec.com/274658.html >.	

Technology Center 2100

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.